enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Information leakage

ENISA Threat Landscape

Overview

A data breach occurs when data, for which an organisation is responsible, is subject to a security incident resulting in a breach of confidentiality, availability or integrity.[1] A data breach frequently causes an information leakage, which is one of the major cyber threats, covering a wide variety of compromised information from personal identifiable information (PII), financial data stored in IT infrastructures to personal health information (PHI) kept in healthcare providers' repositories.

When security breaches are encountered in the headlines of bulletins, blogs, newspapers, and technical reports, the focus is mostly either on adversaries or on the catastrophic failure of the cyber-defence processes and techniques. Nevertheless, the undisputable truth is that, despite the impact or scope of such an event, the breach is usually caused by an individual's action or by an organisational process failure.[2]

__Findings

2.013_ confirmed data disclosures in 2019

During the first half of 2019, the organisations experienced an 11% increase in disclosures compared with 2018.[5,6]

14%_ of all incidents in the financial sector were data disclosures

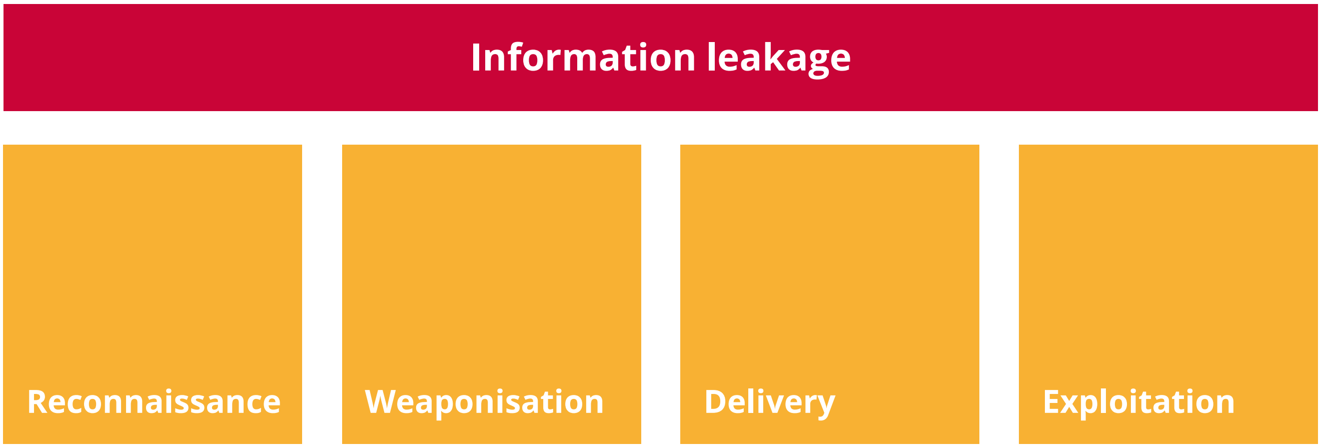
In 47% of them, the victim was a bank.[9]

4,1_ billion data records were exposed globally in the first half of 2019

E-mail and passwords were at the top of the list.[10]

€5,46_ million is the highest cost incurred by healthcare sector[11]

Kill chain



Information leakage

Reconnaissance

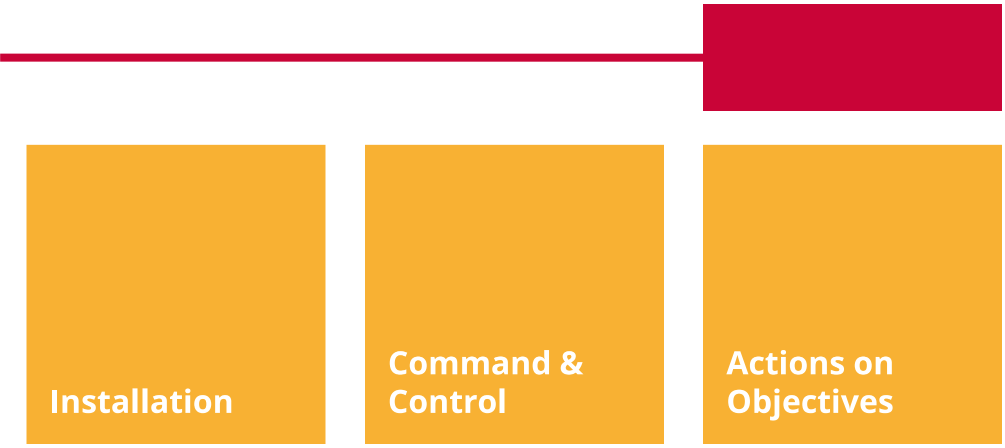
Weaponisation

Delivery

Exploitation

🟥 *Step of Attack Workflow*

🟧 *Width of Purpose*



Installation

Command & Control

Actions on Objectives

The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

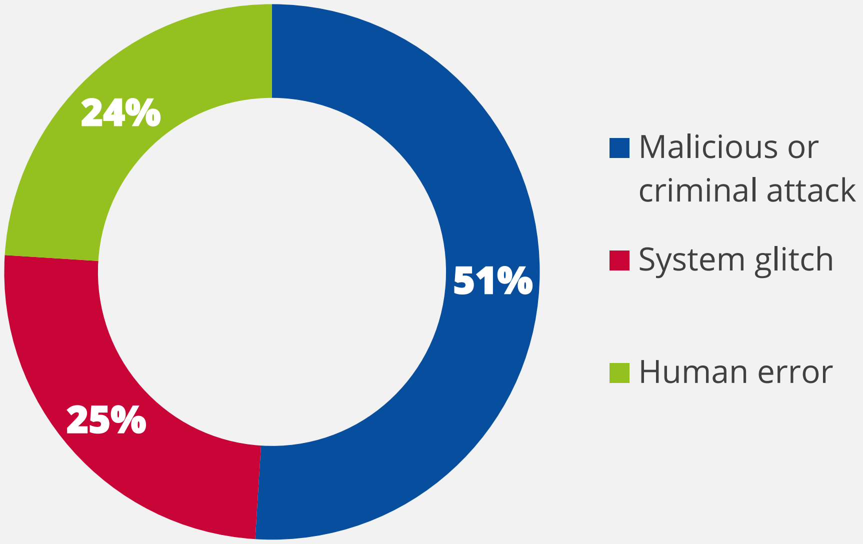
MORE INFORMATION

Incidents

_ Top data leak incidents

- In January 2019, the independent researcher Troy Hunt found 773 million users’ e-mail addresses and passwords in the **cloud-storage service MEGA**. Hunt named this breached dataset as ‘Collection#1’ and notified the service ‘Have I been Pwned?’ so it could notify the account owners to change their login passwords for accessing MEGA platform.[12] In the same month, rogue individuals released personal details, private communications, and financial information of hundreds of **German politicians**, with targets representing every political party but the far-right AfD (Alternative für Deutschland).[6]
- In February 2019, more than 61 million accounts were culled from 16 websites and put up for sale on the dark web. Site owners of Whitepages, Dubsmash, Armor Games, 500px and ShareThis saw their users' stolen data sold for less than US $20.000 (ca. €17.000) in Bitcoin.[13]
- In March 2019, hundreds of millions of **Facebook** and **Instagram** users saw that their credentials were exposed by the social media company's poor password storage management.[14]
- In April 2019, 12,5 million medical records of pregnant women were exposed in India, because of a leaky government server belonging to a healthcare agency. The medical information exposed was related to the pre-conception and pre-natal diagnostic techniques act, an Indian law passed which that banning pre-natal sex determination in an attempt to prevent Indian families from aborting unborn girls and skewing the sex ratio towards boys.[15]

- In May 2019, **DoorDash**, a food delivery service, suffered a data breach that affected almost 5 million users. The subsequent investigation determined that information such as names, e-mail addresses, delivery addresses, order history, phone numbers and passwords had been accessed. The company said that the last four digits of some consumers' credit cards and bank account numbers had also been accessed.[16]
- In June 2019, the **American Medical Collection Agency (AMCA)** began notifying clients of a system hack that breached the billing and medical data of some of its clients, including 11,9 million records of **Quest Diagnostics**, which is one of the largest blood testing companies in the United States. According to a recent Securities and Exchange Commission 8K filing, a hacker had gained access to the AMCA's system for nearly eight months between 1 August 2018 and March 30 2019.[17]



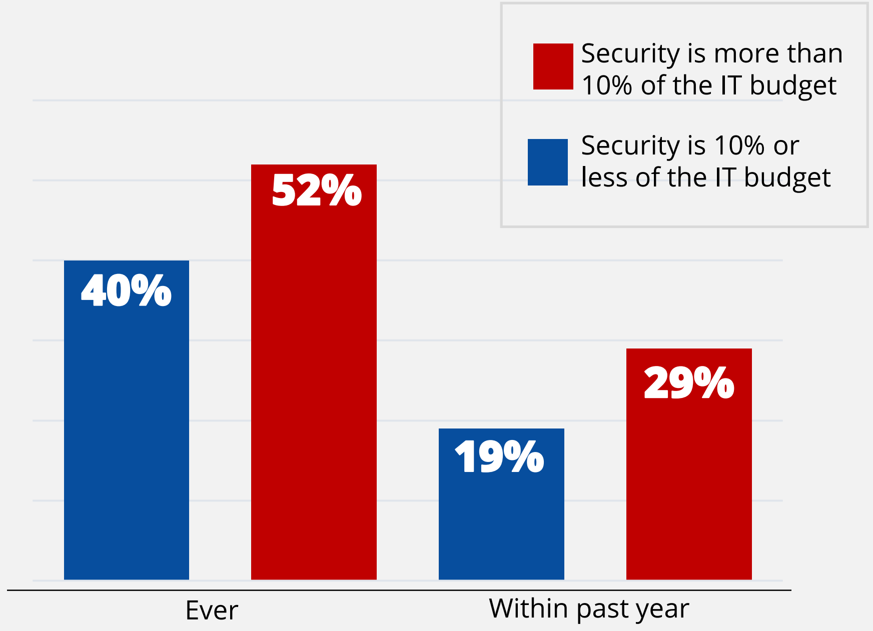
Information disclosure root causes. Source: Ponemon, IBM Security[22]

Incidents

_ Top data leak incidents

- In July 2019, the financial corporation **Capital One** suffered an information leakage that affected 100 million credit card applications, 140.000 social security numbers and 80.000 bank account numbers. Capital One reported that no credit card account numbers or login credentials were exposed. However, the breach exposed names, addresses, postal codes, phone numbers, e-mail addresses and birth dates.[18]
- In August 2019, 160 million records of **MoviePass** were left unencrypted. Because the company's database wasn't password-protected, it left customers' credit card numbers and other details exposed. The database remained online for several days.[19] Meanwhile, a massive leak exposed 27,8 million biometric staff records held by the **British Metropolitan Police, banks and defence contractors**. The database was administered by Suprema, a company that collaborates with the British police.[20,21]
- In September 2019, more than 218 million **'Words with Friends'** player accounts were hacked. The users' database included data from Android and iOS players who had installed the game before September 2. The hacker team 'Gnostic players' accessed information such as players' names, e-mail addresses, login identities and more.[23]
- In October 2019, Adobe left 7,5 million Creative Cloud customer records on an insecure database. The information leakage included the users' e-mail addresses and payment status.[24]
- In November 2019, Facebook gave inappropriate access to the profile data of its 70.000 customers to about 100 app developers. One of them stole the personal data and later used these data to scam them.[25]

- In December 2019, a **Dutch politician** faced 3 years in prison for hacking 100 women’s iCloud accounts and leaking nude pictures. The politician was found to have hacked the women's personal iCloud accounts with credentials found in earlier public database breaches.[26] During the same month, the details of over 10,7 million **Metro-Goldwyn-Mayer (MGM)** resort guests were disclosed on a hacking forum. The leaked information included full customer name, home addresses, phone numbers, e-mail addresses, and birth dates.[27]

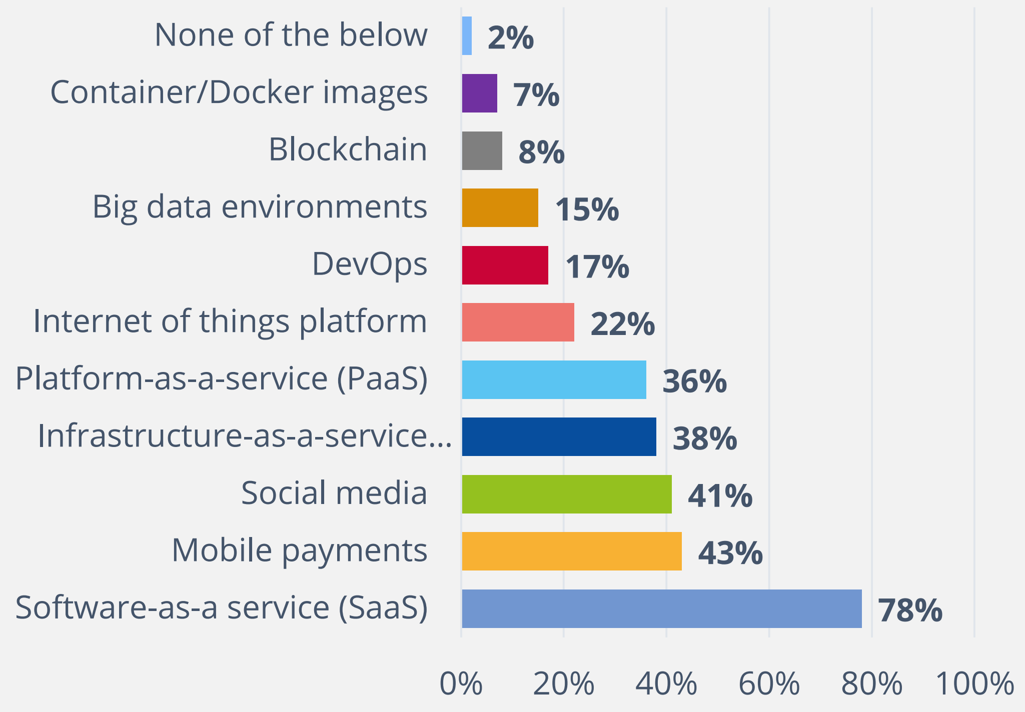


Breach incident rates by level of security spent. Source: CNET[14]

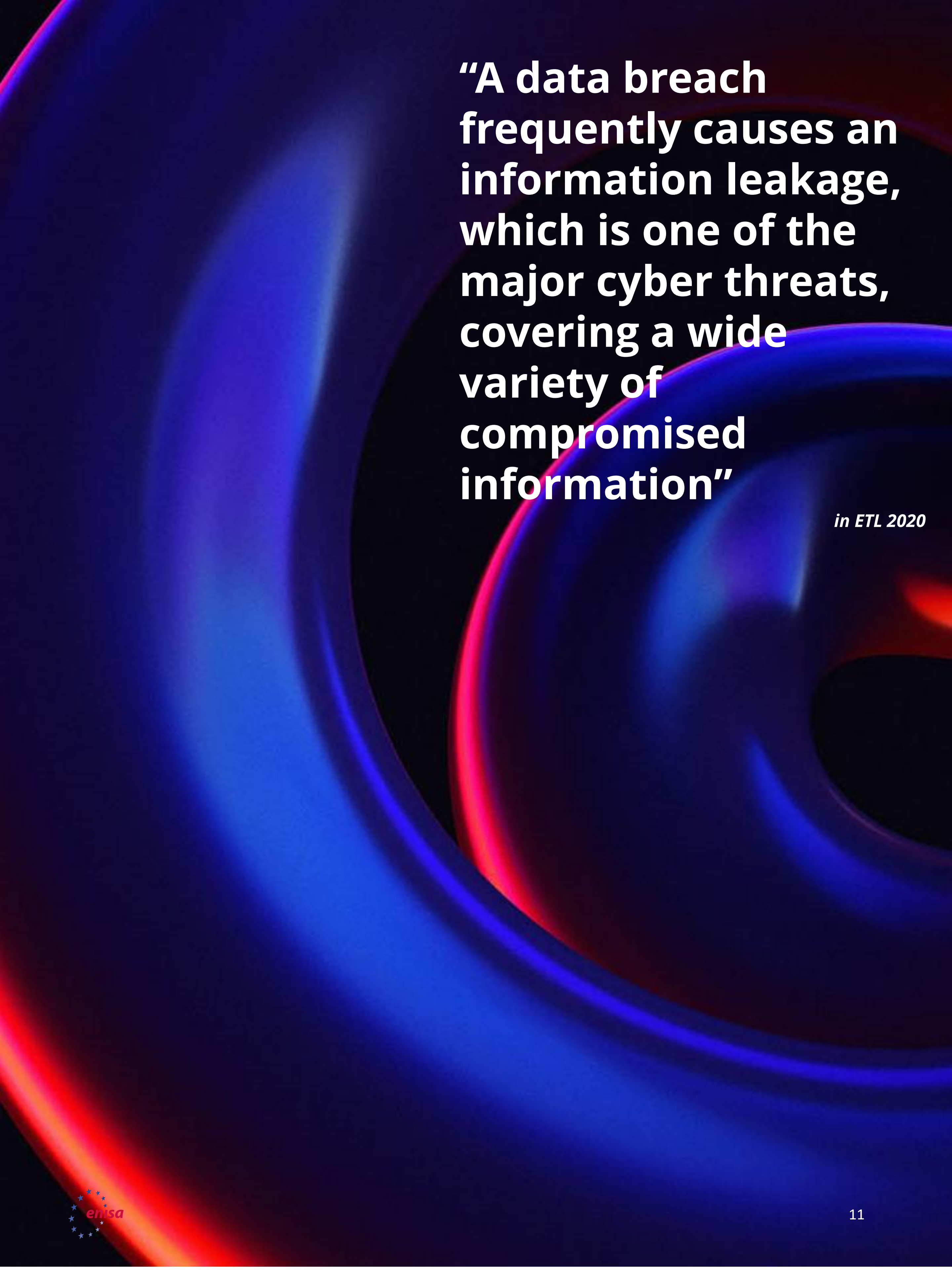
Attack vectors

_How

The primary attack vector in information leakage is insiders. This term is used to describe a person with an interest in 'exfiltrating' important inside information on behalf of a third party. Other common attack vectors used by this threat are misconfigurations, vulnerabilities and human errors.



Types of sensitive or regulated data stored. Source: Thales[40]



“A data breach frequently causes an information leakage, which is one of the major cyber threats, covering a wide variety of compromised information”

in ETL 2020

Mitigation

_Proposed actions

- Anonymise, pseudonymise, minimise and cipher data in accordance with the provisions of the EU GDPR, the California Consumer Privacy Act (CCPA), and the China's Multi-level Protection of Information Security (MLPS 2.0).[28,29,30,31] Always check the regulation commitments for counterpart entities who do not fall under bi- or multi-lateral initiatives.[32, 33,34]
- Store data only on secure IT assets.[35]
- Limit user access privileges under the need-to-know principle.[35,36] Revoke access privileges of anyone who is not an employee.[35]
- Educate and train your organisation's personnel periodically.[35,37]
- Use technology tools to avoid possible data leakages, such as vulnerability scans, malware scans and data loss prevention (DLP) tools. Deploy data and portable system and device encryption, and secure gateways.[36,38]
- A business continuity plan (BCP) is crucial for dealing with a data breach. This plan outlines the type of data being stored and their location, and what potential liabilities could arise when implementing data security and recovery actions. A BCP entails an effective incident response, which aims to address, manage, and rectify the damages caused by such an incident.[39]

“In many cases, companies or organisations are not aware of a data breach happening in their environment because of the sophistication of the attack and sometimes the lack of visibility and classification in their information system.”

in ETL 2020

References

1. “What is a data breach and what do we have to do in case of a data breach?” European Commission. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

2. “The humn factor of cyber security.” CSO. https://www.csoonline.com/article/3504813/the-human-factor-of-cyber-security.html

3. Howard Poston. “Common causes of large breaches (Q1 2019).” May 1, 2019. INFOSEC Institute. https://resources.infosecinstitute.com/common-causes-of-large-breaches/#gref

4. J. Clement. “Average cost of data breaches worldwide from 2014 to 2019.” August 13, 2019. Statista. https://www.statista.com/statistics/987474/global-average-cost-data-breach/

5. “2019 Data Breach Investigations Report.” 2019. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

6. “Cyber Threatscape Report.” 2019. iDefense – Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

7. “Cybercrime will cost businesses over $2 trillion by 2019.” May 12, 2015. Juniper Research https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

8. “How much would a data breach cost your business?.” 2019. IBM. https://www.ibm.com/security/data-breach

9. G. Dautovic. “Top 25 Financial Data Breach Statistics for 2020.” March 11, 2020. Fortunly. https://fortunly.com/statistics/data-breach-statistics#gref

10. Davey Winder**.**“Data Breaches Expose 4.1 BIllion Records In First Six Months of 2019.” August 20, 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#40479be4bd54

11. “Cost of a Data Breach Report.” 2019. Ponemon Institute – IBM. https://databreachcalculator.mybluemix.net/executive-summary/

12. Troy Hunt. “The 773 Million Record “Collection #1.” Data Breach” January 17, 2019. Troy Hunt. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

13. Lewis Morgan. “List of data breaches and cyber attacks in February 2019 – 873,919, 635 records leaked.” February 26, 2019. IT Governance. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2019-692853046-records-leaked

14. Rae Hodge. “2019 Data Breach Hall of Shame: These were the biggest data breaches of the year.” December 27, 2019. CNET. https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/

15. Catalin Cimpanu. “Indian govt agency left details of millions of pregnant women exposed online.” April 1, 2019. ZDNet. https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

16. Shelby Brown. “DoorDash data breach affected 4.9M customers, drivers, merchants.” September 26, 2019. CNET. https://www.cnet.com/news/doordash-data-breach-affected-4-9-million-customers-workers-and-merchants/

17. Jessica Davis.“11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach.” June 3, 2019. HealthITSecurity https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach

18. Alfred Ng, Mark Serrels. “Capital One data breach involves 100 million credit card applications.” July 30, 2019. CNET. https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/

19. Shelby Brown. “Data breaches timeline: EasyJet cyberattack exposes over 9M people, and more.” May 19.2020. CNET. https://www.cnet.com/how-to/equifax-mgm-resorts-beyond-every-major-security-breach-and-data-hack-update/

20. Josh Taylor. “Major breach found in biometrics system used by banks, UK police and defence firms .” August 14.2019. The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

21. Guy Fawkes."Report:Data Breach in Biometric Security Platform Affecting Millions of Users." June 16, 2020. vpnMentor. ttps://www.vpnmentor.com/blog/report-biostar2-leak/

22. "Cost of a Data Breach Report." 2019. Ponemon - IBM Security. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

23. Oscar Gonzalez. "Zynga data breach exposed 200 million Words with Friends players." October 1, 2019. CNET. https://www.cnet.com/news/people-rarely-change-their-passwords-after-a-data-breach-study-says/

24. John E Dunn."Adobe database exposes 7.5 million Creative Cloud users." October 28, 2019. Naked Security. https://nakedsecurity.sophos.com/2019/10/28/adobe-database-exposes-7-5-million-creative-cloud-users/

25. "Insider Sold 68K Customer Records to Scammers: Trend Micro." November 8, 2019. CISOMAG. https://www.cisomag.com/insider-sold-68k-customer-records-to-scammers-trend-micro/

26. Catalin Cimpanu. "Dutch politician faces three years in prison for hacking iCloud accounts and leaking nudes." December 3, 2019. ZDNet. https://www.zdnet.com/article/dutch-politician-faces-three-years-in-prison-for-hacking-icloud-accounts-and-leaking-nudes/

27. Corinne Reichert. "MGM Resorts confirms data breach of 10.7 million guests." February 19, 2020 https://www.cnet.com/news/mgm-resorts-confirms-data-breach-of-10-million-guest-accounts/

28. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." April 27, 2016. European Parliament, Council of the European Union. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679

29. "AB-375 Privacy: personal information: businesses, Assembly Bill No. 375, Chapter 55." June 29, 2018. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

30. Shrub Chandrasekaran, Justin Fishman. "China's Cybersecurity Future and its Impact on U.S. Business." October 31, 2019. Jolt Digest. https://jolt.law.harvard.edu/digest/chinas-cybersecurity-future-and-its-impact-on-u-s-business

31. Reed Smith LLP."MLPS 2.0: China's enhanced data security multi-level protection scheme and related enforcement updates ." October 9, 2019. Lexology. https://www.lexology.com/library/detail.aspx?g=36c6932b-bf41-4e08-b430-e3bc839a2328

32. "Data protection if there's no Brexit deal." September 13, 2018. GOV. UK, Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

33. Eduardo Ustaran, "Brexit and data protection: Laying the odds." September 21, 2018. Privacy Perspectives, iapp. https://iapp.org/news/a/brexit-and-data-protection-laying-the-odds/

34. Ibrahim Hasan. "Data protection and Brexit." September 5, 2016. Gazette. https://www.lawgazette.co.uk/legal-updates/data-protection-and-brexit/5057412.article

35. Eric Dosal. "5 Tips to Prevent Data Leakage at Your Company." March 15, 2018. Compuquip Cybersecurity.https://www.compuquip.com/blog/5-tips-to-prevent-data-leakage-at-your-company

36. "10 ways to protect sensitive business data." October 28, 2019. QuoStar. https://www.quostar.com/blog/10-tips-to-help-prevent-a-data-leak/

37. "Annual Cybersecurity Report." 2018. Cisco https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

38. "Cybercrime tactics and techniques: Q2 2018." 2018. Malwarebytes Labs

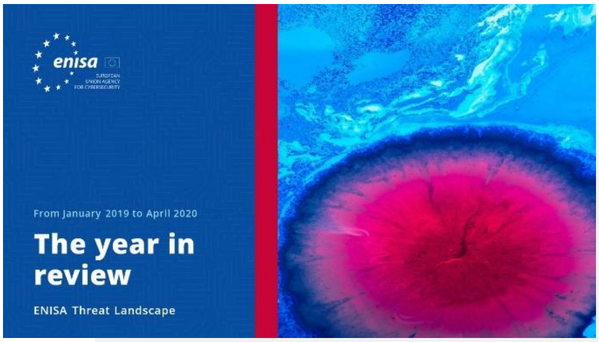
https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf

39. Mona Mangat."81 Eye-Opening Data Breach Statistics for 2020." January 27, 2020. phoenixNAP. https://phoenixnap.com/blog/data-breach-statistics

40. "2020 Data Threat Report – Global Edition." 2020. Thales Group. https://www.thalesesecurity.com/2020/data-threat-report

41. Oscar Gonzalez. "Zynga data breach exposed 200 million Words with Friends players." Pctober 1, 2019. C|net.https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/

Related



From January 2019 to April 2020

The year in review

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **The year in review**

A summary on the cybersecurity trends for the period between January 2019 and April 2020.

From January 2019 to April 2020

ENISAs' list of top 15 threats

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **List of Top 15 Threats**

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

From January 2019 to April 2020

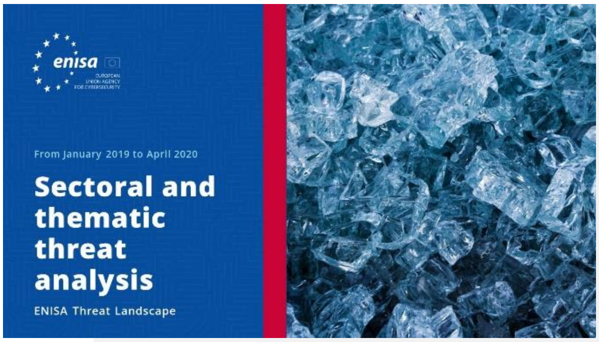
Research topics

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **Research topics**

Recommendations on research topics from various quadrants in cybersecurity and cyberthreat intelligence.



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

Sectoral and thematic threat analysis

ENISA Threat Landscape

ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.

READ THE REPORT

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

Emerging trends

ENISA Threat Landscape

ENISA Threat Landscape Report **Emerging trends**

Main trends in Cybersecurity observed between January 2019 and April 2020.

READ THE REPORT

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

Cyberthreat intelligence overview

ENISA Threat Landscape

ENISA Threat Landscape Report **Cyber Threat Intelligence overview**

The current state of play of cyberthreat intelligence in the EU.

READ THE REPORT

About

_ The agency

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors
Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

Editors
Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

Contact
For queries on this paper, please use enisa.threat.information@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu